Final draft ETSI EN 300 175-7 V2.3.0 (2010-02)

European Standard (Telecommunications series)

Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-edaa0585f2e9/etsi-en-300-175-7-v2.3.1-2010-06

Reference
REN/DECT-000254-7

Keywords
DECT, IMT-2000, mobility, radio, TDD, TDMA

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/a8e900-a6b4-ab6-d8e5-e85512e/etsi-en-300-175-7-v2.3.1-2010-06

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2010.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 8
Foreword 8
Introduction 9
1 Scope 12
2 References 12
2.1 Normative references 13
2.2 Informative references 13
3 Definitions and abbreviations 14
3.1 Definitions 14
3.2 Abbreviations 14
4 Security architecture 15
4.1 Background 15
4.2 Security services 15
4.2.1 Authentication of a PT 15
4.2.2 Authentication of an FT 15
4.2.3 Mutual authentication 16
4.2.4 Data confidentiality 16
4.2.5 User authentication 16
4.3 Security mechanisms 16
4.3.1 Authentication of a PT 16
4.3.2 Authentication of an FT 17
4.3.3 Mutual authentication 18
4.3.4 Data confidentiality 19
4.3.4.1 Derived Cipher Key (DCK) 19
4.3.4.2 Static Cipher Key (SCK) 19
4.3.4.3 Default Cipher Key (DefCK) 19
4.3.5 User authentication 20
4.4 Cryptographic parameters and keys 20
4.4.1 Overview 20
4.4.2 Cryptographic parameters 20
4.4.3 Cryptographic keys 21
4.4.3.1 Authentication key K 22
4.4.3.2 Authentication session keys KS and KS' 22
4.4.3.3 Cipher key CK 23
4.5 Security processes 23
4.5.1 Overview 23
4.5.2 Derivation of authentication key, K 23
4.5.2.1 K is derived from UAK 24
4.5.2.2 K is derived from AC 24
4.5.2.3 K is derived from UAK and UPI 24
4.5.3 Authentication processes 24
4.5.3.1 Processes for the derivation of KS and KS' 25
4.5.3.2 Processes for the derivation of DCK, RES1 and RES2 25
4.5.4 Key stream generation 26
4.6 Combinations of security services 26
5 Algorithms for security processes 27
5.1 Background 27
5.1.1 A algorithm 27
5.2 Derivation of session authentication key(s) 27
5.2.1 A11 process 27
5.2.2 A21 process 28
5.3 Authentication and cipher key generation processes 28
5.3.1 A12 process 28
5.3.2 A22 process 28

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-eda05851e9/etsi-en-300-175-7-v2.3.1-2010-06

6 Integration of security 29
6.1 Background 29
6.2 Association of keys and identities 29
6.2.1 Authentication key 29
6.2.1.1 K is derived from UAK 29
6.2.1.2 K derived from AC 29
6.2.1.3 K derived from UAK and UPI 30
6.2.2 Cipher keys 30
6.3 NWK layer procedures 30
6.3.1 Background 30
6.3.2 Authentication exchanges 31
6.3.3 Authentication procedures 32
6.3.3.1 Authentication of a PT 32
6.3.3.2 Authentication of an FT 32
6.3.4 Transfer of Cipher Key, CK 32
6.3.5 Re-Keying 32
6.3.6 Encryption with Default Cipher Key 33
6.4 MAC layer procedures 33
6.4.1 Background 33
6.4.2 MAC layer field structure 33
6.4.3 Data to be encrypted 34
6.4.4 Encryption process 35
6.4.5 Initialization and synchronization of the encryption process 37
6.4.6 Encryption mode control 37
6.4.6.1 Background 37
6.4.6.2 MAC layer messages 38
6.4.6.3 Procedures for switching to encrypt mode 38
6.4.6.4 Procedures for switching to clear mode 43
6.4.6.5 Procedures for re-keying 44
6.4.7 Handover of the encryption process 45
6.4.7.1 Bearer handover, uninterrupted ciphering 46
6.4.7.2 Connection handover, uninterrupted ciphering 46
6.4.7.3 External handover - handover with ciphering 46
6.4.8 Modifications for half and long slot specifications 46
6.4.8.1 Background 46
6.4.8.2 MAC layer field structure 47
6.4.8.3 Data to be encrypted 47
6.4.8.4 Encryption process 47
6.4.8.5 Initialization and synchronization of the encryption process 47
6.4.8.6 Encryption mode control 48
6.4.8.7 Handover of the encryption process 48
6.4.9 Modifications for double slot specifications 48
6.4.9.1 Background 48
6.4.9.2 MAC layer field structure 48
6.4.9.3 Data to be encrypted 49
6.4.9.4 Encryption process 49
6.4.9.5 Initialization and synchronization of the encryption process 50
6.4.9.6 Encryption mode control 50
6.4.9.7 Handover of the encryption process 50
6.4.10 Modifications for multi-bearer specifications 50
6.4.11 Modifications for 4-level, 8-level, 16-level and 64-level modulation formats 51
6.4.11.1 Background 51
6.4.11.2 MAC layer field structure 51
6.4.11.3 Data to be encrypted 51
6.4.11.4 Encryption process 51
6.4.11.5 Initialization and synchronization of the encryption process 57
6.4.11.6 Encryption mode control 57
6.4.11.7 Handover of the encryption process 57
6.5 Security attributes 57
6.5.1 Background 57
6.5.2 Authentication protocols 58
6.5.2.1 Authentication of a PT 58

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-edaa0585f2e9/etsi-en-300-175-7-v2.3.1-2010-06

6.5.2.2 Authentication of an FT 59
6.5.3 Confidentiality protocols 60
6.5.4 Access-rights protocols 62
6.5.5 Key numbering and storage 62
6.5.5.1 Authentication keys 62
6.5.5.2 Cipher keys 63
6.5.6 Key allocation 64
6.5.6.1 Introduction 64
6.5.6.2 UAK allocation 64

7 Use of security features 65
7.1 Background 65
7.2 Key management options 66
7.2.1 Overview of security parameters relevant for key management 66
7.2.2 Generation of authentication keys 67
7.2.3 Initial distribution and installation of keys 67
7.2.4 Use of keys within the fixed network 68
7.3 Confidentiality service with a Cordless Radio Fixed Part (CRFP) 73
7.3.1 General 73
7.3.2 CRFP initialization of PT cipher key 73

Annex A (informative): Security threats analysis 74

A.1 Introduction 74

A.2 Threat A - Impersonating a subscriber identity 75

A.3 Threat B - Illegal use of a handset (PP) 75

A.4 Threat C - Illegal use of a base station (FP) 75

A.5 Threat D - Impersonation of a base station (FP) 76

A.6 Threat E - Illegally obtaining user data and user related signalling information 76

A.7 Conclusions and comments 77

Annex B (informative): Security features and operating environments 79

B.1 Introduction 79

B.2 Definitions 79

B.3 Enrolment options 79

Annex C (informative): Reasons for not adopting public key techniques 81

Annex D (informative): Overview of security features 82

D.1 Introduction 82

D.2 Authentication of a PT 82

D.3 Authentication of an FT 83

D.4 Mutual authentication of a PT and an FT 83
D.4.1 Direct method 83
D.4.2 Indirect method 1 83
D.4.3 Indirect method 2 83

D.5 Data confidentiality 83
D.5.1 Cipher key derivation as part of authentication 84
D.5.2 Static cipher key 84

D.6 User authentication 84

D.7 Key management in case of roaming 84
D.7.1 Introduction 84
D.7.2 Use of actual authentication key K 84

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-edaa058d2e9/etsi-en-300-175-7-v2.3.1-2010-06

D.7.3 Use of session keys....85
D.7.4 Use of precalculated sets....85

Annex E (informative): Limitations of DECT security....86

E.1 Introduction....86
E.2 Protocol reflection attacks....86
E.3 Static cipher key and short Initial Vector (IV)....86
E.4 General considerations regarding key management....87
E.5 Use of a predictable challenge in FT authentication....87

Annex F (informative): Security features related to target networks....88

F.1 Introduction....88
F.1.1 Notation and DECT reference model....88
F.1.2 Significance of security features and intended usage within DECT....88
F.1.3 Mechanism/algorithm and process requirements....89
F.2 PSTN reference configurations....90
F.2.1 Domestic telephone....90
F.2.2 PBX....91
F.2.3 Local loop....93
F.3 ISDN reference configurations....94
F.3.1 Terminal equipment....94
F.3.2 Network termination 2....95
F.3.3 Local loop....95
F.4 X.25 reference configuration....95
F.4.1 Data Terminal Equipment (DTE)....95
F.4.2 PAD equipment....96
F.5 GSM reference configuration....96
F.5.1 Base station substation....96
F.5.2 Mobile station....96
F.6 IEEE 802 reference configuration....96
F.6.1 Bridge....96
F.6.2 Gateway....96
F.7 Public access service reference configurations....97
F.7.1 Fixed public access service reference configuration....97

Annex G (informative): Compatibility of DECT and GSM authentication....98

G.1 Introduction....98
G.2 SIM and DAM functionality....98
G.3 Using an SIM for DECT authentication....99
G.4 Using a DAM for GSM authentication....99

Annex H (informative): DECT Standard Authentication Algorithm (DSAA)....101

Annex I (informative): Void....102

Annex J (informative): DECT Standard Cipher (DSC)....103

Annex K (normative): Clarifications, bit mappings and examples for DSAA and DSC....104

K.1 Ambiguities concerning the DSAA....104
K.2 Ambiguities concerning the DSC DECT-standard cipher....105

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69e90b-a684-4f46-9b56-cdaa05852c9/etsi-en-300-175-7-v2.3.1-2010-06

Annex L (informative): Bibliography 107

Annex M (informative): Change history 108

History 109

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-edaa0585f2e9/etsi-en-300-175-7-v2.3.1-2010-06

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Digital Enhanced Cordless Telecommunications (DECT), and is now submitted for the ETSI standards One-step Approval Procedure.

The present document is part 7 of a multi-part deliverable. Full details of the entire series can be found in part 1 [1].

The following cryptographic algorithms are subject to controlled distribution:

a) DECT Standard Authentication Algorithm (DSAA);

b) DECT Standard Cipher (DSC).

These algorithms are distributed on an individual basis. Further information and details of the current distribution procedures can be obtained from the ETSI Secretariat at the address on the first page of the present document.

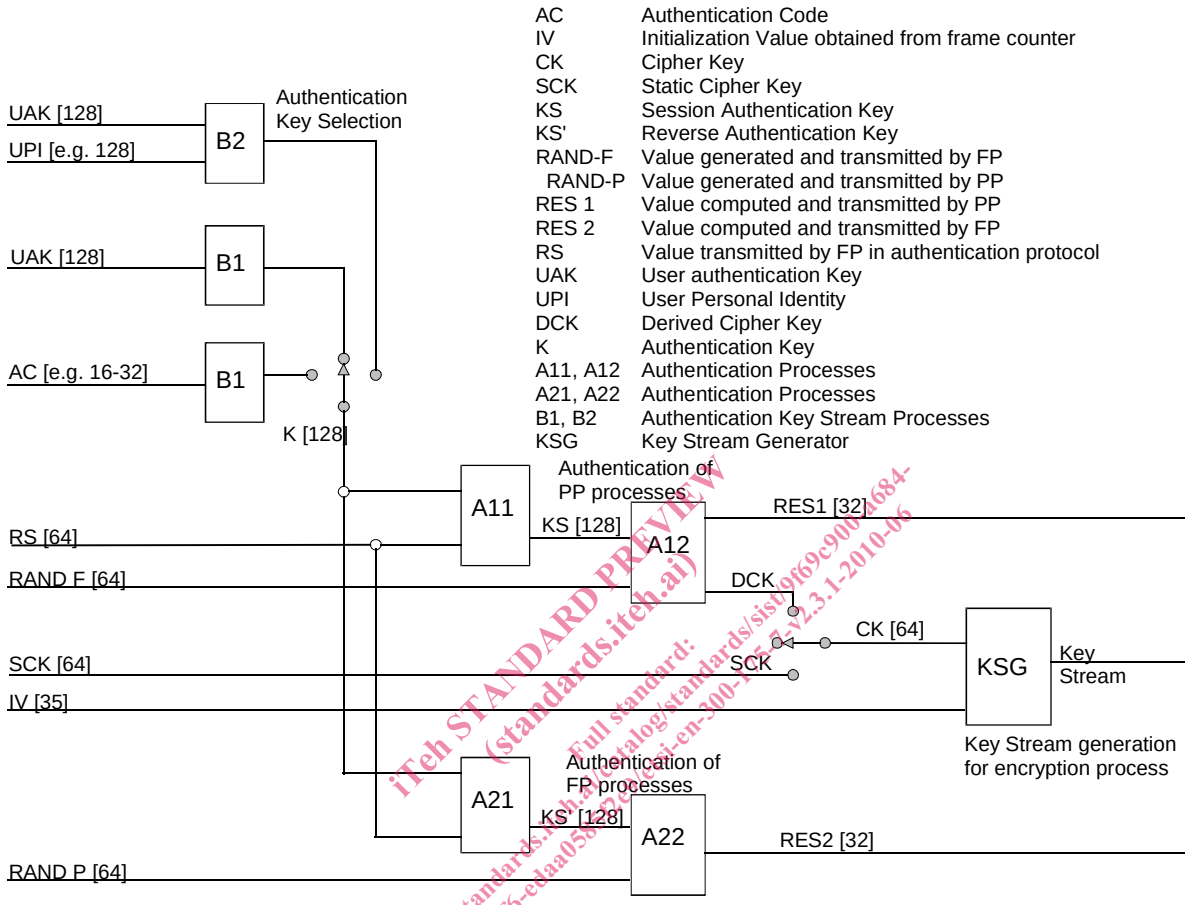
Further details of the DECT system may be found in TR 101 178 [i.1] and ETR 043 [i.2].

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-edaa0585f2e9/etsi-en-300-175-7-v2.3.1-2010-06

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Introduction

The present document contains a detailed specification of the security features which may be provided by DECT systems. An overview of the processes required to provide all the features detailed in the present document is presented in figure 1.



iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-edaa058f2e9e/etsi-en-300-175-7-v2.3.1-2010-06

Figure 1: Overview of DECT security processes

The present document consists of four main clauses (clauses 4 to 7), together with a number of informative/normative and important annexes (A to K). The purpose of this introduction is to briefly preview the contents of each of the main clauses and the supporting annexes.

Each of the main clauses starts with a description of its objectives and a summary of its contents. Clause 4 is concerned with defining a security architecture for DECT. This architecture is defined in terms of the security services which may be offered (see clause 4.2), the mechanisms which shall be used to provide these services (see clause 4.3), the security parameters and keys required by the mechanisms (challenges, keys, etc.), and which shall be passed across the air interface or held within DECT Portable Parts (PPs), Fixed Parts (FPs) or other network entities (for example management centres) (see clause 4.4), the processes which are required to provide the security mechanisms (see clause 4.5) and the recommended combinations of services (see clause 4.6).

Clause 5 is concerned with specifying how certain cryptographic algorithms are to be used for the security processes. Two algorithms are required:

- a key stream generator; and
- an authentication algorithm.

The key stream generator is only used for the encryption process, and this process is specified in clause 4.4. The authentication algorithm may be used to derive authentication session keys and cipher keys, and is the basis of the authentication process itself. The way in which the authentication algorithm is to be used to derive authentication session keys is specified in clause 5.2. The way in which the algorithm is to be used to provide the authentication process and derive cipher keys is specified in clause 5.3.

Neither the key stream generator nor the authentication algorithm is specified in the present document. Only their input and output parameters are defined. In principle, the security features may be provided by using appropriate proprietary algorithms. The use of proprietary algorithms may, however, limit roaming in the public access service environment, as well as the use of PPs in different environments.

For example, for performance reasons, the key stream generator will need to be implemented in hardware in PPs and FPs. The use of proprietary generators will then limit the interoperability of systems provided by different manufacturers.

Two standard algorithms have been specified. These are the DECT Standard Authentication Algorithm (DSAA, see annex H) and the DECT Standard Cipher (DSC, see annex J).

Because of the confidential nature of the information contained in them, these annexes are not included in the present document. However, the algorithms will be made available to DECT equipment manufacturers. The DSAA may also need to be made available to public access service operators who, in turn, may need to make it available to manufacturers of authentication modules.

Clause 6 is concerned with integrating the security features into the DECT system. Four aspects of integration are considered. The first aspect is the association of user security parameters (in particular, authentication keys) with DECT identities. This is the subject of clause 6.2. The second aspect of integration is the definition of the NWK layer protocol elements and message types needed for the exchange of authentication parameters across the air interface. This is dealt with in clause 6.3. The MAC layer procedures for the encryption of data passed over the air interface are the subject of clause 6.4. Finally, clause 6.5 is concerned with security attributes which DECT systems may support, and the NWK layer messages needed to enable PPs and FPs to identify which security algorithms and keys will be used to provide the various security services.

iTeh STANDARD PREVIEW
iTeh Standards (https://standards.iteh.ai)
Document Preview
ETSI EN 300 175-7 V2.3.0 (2010-02)

Clause 7 is concerned with key management issues. Careful management of keys is fundamental to the effective operation of a security system, and clause 7.2 is intended to provide guidance on this subject. The clause includes an explanation of how the DECT security features may be supported by different key management options.

For example, schemes which allow authentication keys to be held in a central location within a public access service network are described, as are schemes which allow authentication keys to be derived locally in public access service base stations. The clause is very much less specific than the other clauses in the present document. This is because the key management issues discussed are not an integral part of the CI. In the end it is up to network operators and service providers to decide how they are going to manage their cryptographic keys. The present document can at best provide some suggestions and guidelines.

The main text is supplemented by a set of informative annexes. There are two types of annex. Those of the first type provide background information justifying the inclusion of a particular service, or the use of a particular type of mechanism in the security features. Those of the second type provide guidance on the use and management of certain of the security features. The content of each of the annexes is briefly reviewed below.

Annex A contains the results of a security threats analysis which was undertaken prior to designing the DECT security features.

Annex B is concerned with the impact of the security features on roaming, in particular with the concurrent use of a PP in public access service, wireless Private Branch eXchange (PBX) and residential environments.

Annex C is provided for background information. It contains a justification for some of the decisions taken by EG-1, for example, why symmetric rather than public key (asymmetric) cryptographic mechanisms were selected.

Annex D provides an overview of the DECT security features specified in the present document.

No security system is perfect, and annex E discusses the limitations of the DECT security features.

Annex F relates the security features specified in the present document to the DECT environments identified in TR 101 178 [i.1]. Each of the local networks identified in the reference model is considered in turn. For each of these networks a security profile is suggested. The networks considered are Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), ITU-T Recommendation X.25 [i.3], Global System for Mobile communications (GSM), Local Area Networks (LANs) and public access service.

Annex G consists of a brief discussion of the compatibility of DECT and GSM authentication. In particular, the concept of a DECT Authentication Module (DAM) is considered and its functionality compared with the functionality of the GSM Subscriber Interface Module (SIM).

Annex H refers to the DECT Standard Authentication Algorithm.

Annex J refers to the DECT Standard Cipher.

Annex K contains normative clarifications, bit mappings and examples for DSAA and DSC.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69c900-a684-4f46-9bf6-edaa0585f2e9/etsi-en-300-175-7-v2.3.1-2010-06

1 Scope

The present document is one of the parts of the specification of the Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI).

The present document specifies the security architecture, the types of cryptographic algorithms required, the way in which they are to be used, and the requirements for integrating the security features provided by the architecture into the DECT CI. It also describes how the features can be managed and how they relate to certain DECT fixed systems and local network configurations.

The security architecture is defined in terms of the security services which are to be supported at the CI, the mechanisms which are to be used to provide the services, and the cryptographic parameters, keys and processes which are associated with these mechanisms.

The security processes specified in the present document are each based on one of two cryptographic algorithms:

- an authentication algorithm; and
- a key stream generator.

The architecture is, however, algorithm independent, and either the DECT standard algorithms, or appropriate proprietary algorithms, or indeed a combination of both can, in principle, be employed. The use of the employed algorithm is specified in the present document.

Integration of the security features is specified in terms of the protocol elements and processes required at the Network (NWK) and Medium Access Control (MAC) layers of the CI.

The relationship between the security features and various network elements is described in terms of where the security processes and management functions may be provided.

The present document does not address implementation issues. For instance, no attempt is made to specify whether the DSAA should be implemented in the PP at manufacture, or whether the DSAA or a proprietary authentication algorithm should be implemented in a detachable module. Similarly, the present document does not specify whether the DSC should be implemented in hardware in all PPs at manufacture, or whether special PPs should be manufactured with the DSC or proprietary ciphers built into them. The security architecture supports all these options, although the use of proprietary algorithms may limit roaming and the concurrent use of PPs in different environments.

The present document includes New Generation DECT, a further development of the DECT standard introducing wideband speech, improved data services, new slot types and other technical enhancements.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f69f690-a684-4fd6-9f66-edad95b5b9d4/etsi-en-300-175-7-v2.3.1-2010-02

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

[2] ETSI EN 300 175-2: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL)".

[3] ETSI EN 300 175-3: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".

[4] Void.

[5] ETSI EN 300 175-5: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".

[6] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[7] Void.

[8] Void.

[9] ETSI TS 100 977: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface (3GPP TS 11.11 Release 1999)".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9f0c900-a684-4f46-9bf6-adaa0585f8e9/etsi-en-300-175-7-v2.3.0-2010-06

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TR 101 178: "Digital Enhanced Cordless Telecommunications (DECT); A High Level Guide to the DECT Standardization".

[i.2] ETSI ETR 043: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Services and facilities requirements specification".

[i.3] ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

[i.4] ETSI ETR 056: "Digital Enhanced Cordless Telecommunications (DECT); System description document".

[i.5] IEEE 802: "Standard for Local and Metropolitan Area Networks: Overview and Architecture".